第 3 章 同余方程

本章重点介绍一次同余方程及一次同余方程组的解的情况及具体求解的方法，其中一次同余方程组，我们主要介绍了著名的孙子定理的求解方法．而对于一般的同余方程，仅大体介绍了一般的求解过程．对于二次同余数方程的解，我们仅考虑素数模的情况，通常称为素数模的二次剩余问题．最后我们介绍了一个与二次剩余有关的数论函数 Legendre 符号，从而定义了更为一般的数论函数 Jacobi 符号．

本章的内容不仅在初等数论中构成了同余理论的核心内容，而且也构成了公钥密码学中多数密码算法的主要内容，因此同余方程在许多密码算法的设计与分析技术中占有重要的地位，如求解一次同余方程是许多密码算法加、解密甚至破译的最基本的运算内容之一；孙子定理不仅是多种密码算法的运算内容之一，而且可直接应用于设计具有特殊形式的密码算法；二次剩余、Jacobi 符号可以用于素检测与设计伪随机生成器等．总之，该部分内容也构成了公钥密码算法的主要运算内容．

§1 一元高次同余方程的概念

本节主要介绍了一般的同余方程及其相关的概念，并简单介绍了同余方程的简化形式．值得注意的是，如果不加特别说明，同余方程一般指一元同余方程．

定义 1 设 $f(x)$ 为整系数多项式，

$$f(x)\equiv a_n x^n+....+a_1 x+a_0 (\mathrm{mod} m),$$

则含有变量 x 的同余式

$$f(x)\equiv 0(\mathrm{mod} m) \tag{1}$$

叫做**模 m 的同余方程.** 若整数 c 满足

$$f(c)\equiv 0(\mathrm{mod} m), \tag{2}$$

则 c 叫做**同余方程 $f(x)\equiv 0(\mathrm{mod} m)$ 的解.**

显然，若 c 是同余方程 $f(x)\equiv 0(\mathrm{mod} m)$ 的解，则同余类 $c \bmod m$ 中任意整数都是解，我们把同余类 $c \bmod m$ 称为同余方程 $f(x)\equiv 0(\mathrm{mod} m)$ 的一个解，所有模 m 两两不同余的解的个数，称为**同余方程 $f(x)\equiv 0(\mathrm{mod} m)$ 的解数.**

定义 2　若 $m \nmid a_n$，则同余方程的次数为 n；若 $m \mid a_j$，　$k+1 \le j \le n$，　$m \nmid a_k$，则同余方程的次数为 k.

从定义 2 知，同余方程（1）的次数不一定等于多项式 $f(x)$ 的次数.

自然，对于模 m 的同余方程的解的个数最多有 m 个，我们可以通过验证的一组完全剩余系来解同余方程，也可通过恒等变形来化简同余方程. 主要的几种恒等变形如下：

性质 1　若 $f(x) \equiv g(x) (\mathrm{mod}\, m)$，则同余方程

$$f(x) \equiv 0 (\mathrm{mod}\, m)$$

与同余方程

$$g(x) \equiv 0 (\mathrm{mod}\, m)$$

的解和解数相同.

性质 2 如果

$$f(x) = q(x)h(x) + r(x)$$

且同余方程 $h(x) \equiv 0 (\mathrm{mod}\, m)$ 为恒等同余式，即方程的解数为 m，则同余方程（1）与同余方程

$$r(x) \equiv 0 (\mathrm{mod}\, m)$$

解与解数相同.

如果 $h(x)$ 的次数 ≥ 1，则一定存在 $q(x), r(x)$，并且 $r(x)$ 的次数小于 $h(x)$ 的次数.

利用恒等同余式降低同余方程的次数，关键是找模 m 的恒等同余式.　如果 m 为素数 p，利用 Fermat-Euler 定理，易知

$$h(x) = x^p - x \equiv 0 (\mathrm{mod}\, p)$$

为恒等同余式.

性质 3 设 $(a, m) = 1$,　同余方程

$$f(x) \equiv 0 (\mathrm{mod}\, m)$$

和同余方程

$$af(x) \equiv 0 (\mathrm{mod}\, m)$$

等价.

特别地，如果$(a_n,m)=1$，则同余方程（1）可以化为首系为 1 的同余方程

$$(a_n)^{-1}f(x)\equiv 0(\mathrm{mod}m).$$

根据同余的性质，可得到一个同余方程有解的必要条件

定理 1 若整数$d|m,$ 那么同余方程

$$f(x)\equiv 0(\mathrm{mod}\,m)$$

有解的必要条件为

$$f(x)\equiv 0(\mathrm{mod}\,d)$$

有解.

这个定理可以很方便地用来判定一个方程无解.

例 1 求解同余方程$4x^2+27x-9\equiv 0 \pmod{15}$.

解 15 的素因子只有 3、5，在模 1 5 的剩余系中只有

$$f(3)\equiv 3\equiv 0(\mathrm{mod}\,3)\text{；}$$

但是

$$f(3)\equiv -7\not\equiv 0(\mathrm{mod}\,5)\text{，}$$

从而此同余方程无解.

例 2 求同余方程$5x^3-3x^2+3x-1\equiv 0(\mathrm{mod}11)$.

解 取模 11 的绝对最小完全剩余系$-5,-4,-3,-2,-1,0,1,2,3,4,5$，直接计算知

$x=2$ 是解．所以这个同余方程的解是$x\equiv 2(\mathrm{mod}11)$.

例 2 求同余方程

$$3x^{15}-x^{13}-x^{12}-x^{11}-3x^5+6x^3-2x^2+2x-1\equiv 0(\mathrm{mod}11).$$

解 利用同余恒等式$x^{11}\equiv x(\mathrm{mod}11)$，由多项式除法得

$$3x^{15}-x^{13}-x^{12}-x^{11}-3x^5+6x^3-2x^2+2x-1$$

$$=(x^{11}-x)(3x^4-x^2-x+1)+5x^2-3x^2+3x-1(\mathrm{mod}11)\text{，}$$

所以原同余方程与同余方程

$$5x^3-3x^2+3x-1\equiv 0(\mathrm{mod}11)$$

同解，由例 2 可知同余方程的解为 $x\equiv 2(\mathrm{mod}11)$.

§2 一次同余方程

前面简单介绍了一般的同余方程，下面主要讨论一次同余方程

$$ax\equiv b(\mathrm{mod}\,m) \qquad (1)$$

解的情况及求解方法.

定理 1 若 $(a,m)=1$，则同余方程 $ax\equiv b(\mathrm{mod}\,m)$ 有且仅有一个解.

证明 存在性：当 $(a,m)=1$ 时，则存在 a^{-1}，使 $aa^{-1}\equiv 1(\mathrm{mod}\,m)$. 所以

$$x=a^{-1}b(\mathrm{mod}\,m)$$

满足方程.

唯一性：若存在另外一个解 $x'(\mathrm{mod}\,m)$，那么

$$ax=ax'(\mathrm{mod}\,m),$$

因为 $(a,m)=1$，所以

$$x=x'(\mathrm{mod}\,m).$$

证毕.

由 Euler 定理知，若 $(a,m)=1$，

$$a^{-1}=a^{\phi(m)-1}(\mathrm{mod}\,m),$$

所以同余方程（1）的唯一解为

$$x=a^{\phi(m)-1}b(\mathrm{mod}\,m).$$

实际上，利用通过 Euclid 算法求 a^{-1}，然后求解方程（1）的解是较有效的方法.

定理 2 同余方程

$$ax \equiv b(\mathrm{mod}\, m)$$

有解的充要条件是$(a,m)|b$．在有解时，解数等于(a,m)．若x_0是它的一个解，则它的(a,m)个解是

$$x \equiv x_0 + \frac{m}{(a,m)}t(\mathrm{mod}\, m),\quad t = 0,1,\cdots(a,m)-1.$$

证明 必要性：一次同余方程（1）有解，则存在x_1, y_1使得

$$ax_1 = b + my_1,$$

所以$(a,m)|b$.

充分性：设$d=(a,m)$，若$(a,m)|b$成立，由第二章性质4知，同余式

$$ax \equiv b(\mathrm{mod}\, m)$$

成立当且仅当

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\frac{m}{d}\right)$$

成立.

由于$\left(\frac{a}{d},\frac{m}{d}\right)=1$，则

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\frac{m}{d}\right) \qquad (2)$$

有解，从而$ax \equiv b(\mathrm{mod}\, m)$有解，充分性得证.

若x_0是（1）的一个特解，x为（1）的任意解，则$x_0\left(\mathrm{mod}\frac{m}{d}\right)$、$x\left(\mathrm{mod}\frac{m}{d}\right)$均是（2）的唯一解，所以$x \equiv x_0\left(\mathrm{mod}\frac{m}{d}\right)$.

反之，对任意的$x \in Z$，若$x \equiv x_0\left(\mathrm{mod}\frac{m}{d}\right)$，则$x$为（1）的解.

所以，同余方程（1）的所有解为

$$\left(x_0+\frac{m}{d}t\right)(\mathrm{mod}\, m),\quad t=0,...,d-1.$$

上面从理论上给出了同余方程

$$ax\equiv b(\mathrm{mod}\, m)$$

的解与解数，下面我们给出上面同余方程的求解步骤：

1) 通过恒等变形将其变为：

$$a'x\equiv b'(\mathrm{mod}\, m),$$

其中$-m/2<a'\le m/2$，$-m/2<b'\le m/2$.

2) 同余方程

$$a'x\equiv b'(\mathrm{mod}\, m)$$

与不定方程

$$a'x=my+b'$$

同解，所以与

$$my\equiv -b'(\mathrm{mod}|a'|)$$

同解.

3) 若

$$my\equiv -b'(\mathrm{mod}|a'|)$$

的解为$y_0(\mathrm{mod}|a'|)$，则$x_0=(my_0+b')/a'(\mathrm{mod}\, m)$为

$$a'x\equiv b'(\mathrm{mod}\, m)$$

的解.

实际上，上述步骤就是带绝对最小剩余的 Euclid 算法，与求一元一次不定方程的特解相同．下面我们用具体例子来说明.

例 1 解同余方程$17x\equiv 229(\mathrm{mod}\,1540)$.

解 原方程与

$$-7y\equiv 8(\mathrm{mod}\,17)$$

同解，

$$7y\equiv -8(\mathrm{mod}\,17)\Leftrightarrow 3u\equiv -1(\mathrm{mod}\,7)\Leftrightarrow u\equiv -5(\mathrm{mod}\,7).$$

由最后一式逐次返回

$$y \equiv (-17\times 5+8)/7 (\mathrm{mod}\, 17) \equiv -11 (\mathrm{mod}\, 17),$$

$$x \equiv [1540\times(-11)+229]/17 \equiv -983 (\mathrm{mod}\, 1540) \equiv 557 (\mathrm{mod}\, 1540).$$

例 2　解同余方程　$14x \equiv 30 (\mathrm{mod}\, 21)$.

解　$(14, 21) = 7 \nmid 30$，所以方程无解.

§3 一次同余方程组 孙子定理

定义 1 设 $f_i(x)$ 是整系数多项式，$1 \le i \le k$，我们把含有变量 x 的一组同余式

$$f_i(x) \equiv 0 (\mathrm{mod}\, m_i),\ 1 \le i \le k, \tag{1}$$

称为**同余方程组**．若整数 c 同时满足

$$f_i(c) \equiv 0 (\mathrm{mod}\, m_i),\qquad 1 \le i \le k,$$

则称 c 是同余方程组的**解**.

若 c 是同余方程(1)的解，则同余类 $c \bmod m,\ \ m = [m_1, \cdots, m_k]$ 中的任一整数也为同余方程组的一个解，$c \bmod m$ 看作一个解，同余方程组中所有模 m 两两不同余的解的个数称为同余方程组的**解数**.

显然，它也至多有 m 个解，且只要有一个方程无解，则同余方程组无解．下面讨论当 $m_0, \cdots, m_{k-1}$ 是两两既约时，一次同余方程组解的情况.

定理 1（**孙子定理**）设 $m_0, \cdots, m_{k-1}$ 是两两既约的正整数，那么，对任意整数 $a_0, \cdots a_{k-1}$，一次同余方程组

$$x \equiv a_i (\mathrm{mod}\, m_i),\ \ 0 \le i \le k-1, \tag{2}$$

必有解，且解数唯一．这个唯一解是

$$x \equiv M_1 M_1^{-1} a_1 + \cdots + M_k M_k^{-1} a_k (\mathrm{mod}\, m),$$

其中

$$m = m_1 \cdots m_k, \quad m = m_i M_i, \quad (0 \le i \le k-1)$$

以及

$$M_i M_i^{-1} \equiv 1 (\mathrm{mod}\, m_i), \quad (1 \le i \le k-1).$$

证明 先来证

$$x \equiv M_1 M_1^{-1} a_1 + \cdots + M_k M_k^{-1} a_k (\mathrm{mod}\, m)$$

是同余方程（2）的解．由于

$$M_i M_i^{-1} \equiv 1 (\mathrm{mod}\, m_i), \quad m_i \mid M_j, i \ne j,$$

故

$$x \equiv M_i M_i^{-1} a_i \equiv a_i (\mathrm{mod}\, m_i), \quad 0 \le i \le k-1,$$

所以 x 是（2）的解．

下证唯一性．若同余方程有两个解 x_1, x_2，则必有

$$x_1 \equiv x_2 \equiv a_i (\mathrm{mod}\, m_i), \quad 0 \le i \le k-1,$$

所以 $m_i \mid x_1 - x_2, \quad 0 \le i \le k-1,$ 由于 $m_0, \cdots, m_{k-1}$ 两两既约，所以

$$m = [m_0, \cdots, m_{k-1}] = m_0 \cdots m_{k-1}.$$

从而有 $x_1 \equiv x_2 (\mathrm{mod}\, m)$．定理得证．

孙子定理描述的是模 $m_0, \cdots, m_{k-1}$ 是两两互素的条件下的一次同余方程组．我们称满足模 $m_0, \cdots, m_{k-1}$ 是两两互素的方程组（1）称为满足孙子定理条件的方程组．对于一般的一组模 $m_0, \cdots, m_{k-1}$，根据 $m_0, \cdots, m_{k-1}$ 的素分解或者通过求解最大公因子将 $m_0, \cdots, m_{k-1}$ 进行分解，总可以将方程组化为满足孙子定理条件的方程组．

例 3 解同余方程组

$$\begin{cases} x \equiv 2 (\mathrm{mod}\, 3) \\ x \equiv 2 (\mathrm{mod}\, 5) \\ x \equiv -3 (\mathrm{mod}\, 7) \\ x \equiv -2 (\mathrm{mod}\, 13) \end{cases}$$

解 利用孙子定理

$$M_1=455,\ M_2=273,\ M_3=195,\ M_4=105;$$

$$M_1^{-1}=-1,\ M_2^{-1}=2,\ M_3^{-1}=-1,\ M_4^{-1}=1.$$

$$x=455\times(-1)\times 2+273\times 2\times 2+195\times(-1)\times(-3)+105\times 1\times(-2)$$

$$=(-910)+1092+585+(-210)$$

$$=557(\mathrm{mod}1365).$$

例 4 解同余方程组

$$\begin{cases}4x\equiv 14(\mathrm{mod}15)\\ 9x\equiv 11(\mathrm{mod}\,20)\end{cases}$$

解 此方程组中 20 和 15 不既约，所以不能直接用孙子定理，方程组等价于如下方程组

$$\begin{cases}4x\equiv 14(\mathrm{mod}\,5)\\ 4x\equiv 14(\mathrm{mod}\,3)\\ 9x\equiv 11(\mathrm{mod}\,4)\\ 9x\equiv 11(\mathrm{mod}\,5)\end{cases}$$

化简得

$$\begin{cases}x\equiv 1(\mathrm{mod}\,5)\\ x\equiv 2(\mathrm{mod}\,3)\\ x\equiv -1(\mathrm{mod}\,4)\\ x\equiv -1(\mathrm{mod}\,5)\end{cases}$$

第一和第四个方程矛盾，所以方程组无解.

§4 一般同余方程组

上节已经完全解决了一次同余方程及一次同余方程组的求解问题，但对于高次的同余方程没有一般的求解方法．下面我们从理论上简要描述求解一般同余方程的主要步骤.

定理 1 当 $m=m_0m_1\cdots m_k,\quad m_i,0\le i\le k$ 两两互素时，同余方程

$$f(x)\equiv 0(\mathrm{mod}\,m) \qquad (1)$$

与同余方程组

$$f(x)\equiv 0(\mathrm{mod}\, m_i),\quad 0\le i\le k \tag{2}$$

同解.

其证明由同余的性质易得.

由定理 1 知，要求同余方程（1）的解，只要求出同余方程组(2)的解．而求解同余方程组（2）的解需要求解每个同余方程的解 $a_{i1},a_{i2},\cdots a_{il}$．然后对每个 $\{a_{ij_k}\},1\le i\le k,1\le j_k\le l$ 求同余方程组

$$x\equiv a_{ij_k}(\mathrm{mod}\, m_i),1\le i\le k$$

的解，即可得出

$$f(x)\equiv 0(\mathrm{mod}\, m)$$

的解．由此，若 $m=p_0^{\alpha_0}p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}$，剩下的问题是如何求下列方程的解

$$f(x)\equiv 0(\mathrm{mod}\ p_i^{\alpha_i}) \tag{3}$$

定理 2 若 $f(x)\equiv 0(\mathrm{mod}\ p^{\alpha-1})$的解为 $x\equiv c_1,c_2,\cdots c_s(\mathrm{mod}\ p^{\alpha-1})$，则方程

$$f(x)\equiv 0(\mathrm{mod}\ p^{\alpha}) \tag{4}$$

的满足

$$x\equiv c_j(\mathrm{mod}\ p^{\alpha-1}),\quad (1\le j\le s) \tag{5}$$

的解有 $x\equiv c_j+p^{\alpha-1}y(\mathrm{mod}\ p^{\alpha})$ 的形式，其中 y 是

$$f'(c_j)y\equiv -f(c_j)p^{1-\alpha}(\mathrm{mod}\ p) \tag{6}$$

的解.

证 明 若我们已知

$$f(x)\equiv 0(\mathrm{mod}\ p^{\alpha-1})$$

的解 $x\equiv c_1,c_2,\cdots c_s(\mathrm{mod}\ p^{\alpha-1})$，则可推出对于

$$f(x)\equiv 0(\mathrm{mod}\ p^{\alpha})$$

的每个解 a，有且仅有一个 $c_j(1\le j\le s)$满足 $a\equiv c_j(\mathrm{mod}\ p^{\alpha-1})$，从而，

$$f(x)\equiv 0(\mathrm{mod}\, p^{\alpha})$$

的解可表为 $x=c_j+p^{\alpha-1}y$ 的形式.

$$\begin{aligned} f(c_j+p^{\alpha-1}y) &= a_n(c_j+p^{\alpha-1}y)^n+a_{n-1}(c_j+p^{\alpha-1}y)^{n-1}+\cdots+a_1(c_j+p^{\alpha-1}y)+a_0 \\ &= f(c_j)+p^{\alpha-1}f'(c_j)y+A_2p^{2(\alpha-1)}y^2+\cdots+A_np^{n(\alpha-1)}y^n \\ &\equiv f(c_j)+p^{\alpha-1}f'(c_j)y(\mathrm{mod}\, p^{\alpha}) \end{aligned}$$

根据同余的性质，上式即求

$$f'(c_j)y\equiv -f(c_j)p^{1-\alpha}(\mathrm{mod}\, p)$$

的解.

注：（I） $p\nmid f'(c)$. 这时同余方程（6）的解的个数为1. 所以同余方程（4）满足条件（5）的解数为 1.

（II） $p\mid f'(c)$， $p\nmid f(c)p^{1-\alpha}$，即

$$f(c)\not\equiv 0(\mathrm{mod}\, p^{\alpha}),$$

这时同余方程（6）无解，所以同余方程（4）没有满足条件（5）的解.

（III） $p\mid f'(c)$， $p\mid f(c)p^{1-\alpha}$，即

$$f(c)\equiv 0(\mathrm{mod}\, p^{\alpha}),$$

这时同余方程（6）的解数为 p，即

$$y\equiv 0,1,\cdots,p-1(\mathrm{mod}\, p)$$

均为（6）的解，所以同余方程（4）满足条件（5）的解数为 p.

综上所述，只要我们解出模为素数 p 的同余方程

$$f(x)\equiv 0(\mathrm{mod}\, p)$$

的解，就可以通过解一次同余方程，解出模为 $p^2,p^3,\cdots p^{\alpha}$ 的同余方程

$$f(x)\equiv 0(\mathrm{mod}\, p^i),\ 2\le i\le \alpha$$

的解，最终求出

$$f(x)\equiv 0(\mathrm{mod}\, m)$$

的解.

例 1　解同余方程组 $x^2 \equiv 3(\mathrm{mod}11^3)$.

解　模 11^3 的完全剩余系可表示为

$$x = x_0 + x_1 \cdot 11 + x_2 \cdot 11^2，\ -5 \le x_i \le 5,\quad 0 \le i \le 2.$$

我们依次解同余方程

$$(x_0 + \cdots + x_i \cdot 11^i)^2 \equiv 3(\mathrm{mod}11^{i+1})，\ 0 \le i \le 2.$$

当 $i = 0$ 时，解

$$x_0{}^2 \equiv 3(\mathrm{mod}11)$$

得

$$x_0 \equiv \pm 5(\mathrm{mod}11).$$

当 $i = 1$ 时，解

$$(\pm 5 + 11x_1)^2 \equiv 3(\mathrm{mod}11^2)$$

得

$$x_1 \equiv \pm 2(\mathrm{mod}11).$$

当 $i = 2$ 时，解

$$(\pm 5 \pm 2 \times 11 + 11^2 x_2)^2 \equiv 3(\mathrm{mod}11^3)$$

得

$$x_1 \equiv \mp 6(\mathrm{mod}11).$$

所以

$$x = \pm 5 \pm 2 \times 11 \mp 6 \times 11^2 = \pm 699(\mathrm{mod}11^3).$$

例 2　求同余方程 $x^2 = 1(\mathrm{mod}\,2^l)$ 的解.

解　当 $l = 1$ 是，解数为 1，$x \equiv 1(\mathrm{mod}\,2)$.

当 $l = 2$ 时，解数为 2，$x \equiv -1, 1(\mathrm{mod}\,2^2)$.

当 $l \ge 3$ 时，同余方程可写为

$$(x-1)(x+1) \equiv 0(\mathrm{mod}\,2^l).$$

由于 x 是解时，可表为 $x=2y+1,$ 带入上式得

$$4y(y+1)\equiv 0(\mathrm{mod}\,2^{l})$$

即

$$y(y+1)\equiv 0(\mathrm{mod}\,2^{l-2})\,,$$

所以

$$y\equiv 0,-1(\mathrm{mod}\,2^{l-2})\,.$$

因此解 x 必满足

$$x\equiv 1,-1(\mathrm{mod}\,2^{l-1})\,.$$

所以原方程的解为

$$x\equiv 1,1+2^{l-1},-1,-1+2^{l-1}(\mathrm{mod}\,2^{l})\,,$$

解数为 4.

例 3 设素数 $p>2$，求同余方程 $x^{2}\equiv 1(\mathrm{mod}\,p^{l})$.

解 由于 $(x-1,x+1)\mid 2$ 所以上式等价于

$$x-1\equiv 0(\mathrm{mod}\,p^{l})\text{ 或 }x+1\equiv 0(\mathrm{mod}\,p^{l})$$

因此，对任意 $l\geq 1$ 解为 $x\equiv -1,1(\mathrm{mod}\,p^{l})$，解数为 2.

§5 二次剩余

在上一节中，解一般的同余方程最终要归结到解模为素数的同余方程．一般模 m 二次同余方程是最常见的同余方程，这种同余方程的解一般归结为求二次剩余问题．尤其是当 $m=pq$ 或 p 情况，二次剩余在密码学中有极重要的作用，详细情况参看本书最后一章内容．本节我们来讨论一下模为奇素数 p 的二次同余方程．

二次同余方程的一般形式为：

$$ax^{2}+bx+c\equiv 0\left(\mathrm{mod}\,p\right)\qquad(1)$$

若 $\left(p,a\right)=1$，则同余方程（1）可以简化为标准形式：

$$x^2 \equiv d(\mathrm{mod}\, p) \qquad (2)$$

当 $p|d$ 时，同余方程（2）有且仅有一解 $x \equiv 0(\mathrm{mod}\, p)$．因此以下恒假定 $(p,d)=1$．

定义 1 设素数 $p>2$，$(p,d)=1$．如果同余方程（2）有解，则称 d 是模 p 的**二次剩余**；若无解，则称 d 是模 p 的**二次非剩余**.

记模 p 的二次剩余与二次非剩余的全体分别为：

$$QR_p = \{a \mid a \in Z_p^*, \exists x \in Z_p^*, x^2 = a(\mathrm{mod}\, p)\},$$

$$NQR_p = \{a \mid a \in Z_p^*, \forall x \in Z_p^*, x^2 \neq a(\mathrm{mod}\, p)\}.$$

定理 2. 1 模 p 的既约剩余系中，二次剩余、二次非剩余各占一半，即

$$|QR_p| = |NQR_p| = (p-1)/2.$$

证明 若 d 是模 p 的二次剩余，则 d 必为

$$\left(-\frac{p-1}{2}\right)^2, \left(-\frac{p-1}{2}+1\right)^2, \cdots, (-1)^2, 1^2, \cdots, \left(\frac{p-1}{2}-1\right)^2, \left(\frac{p-1}{2}\right)^2 (\mathrm{mod}\, p)$$

中一个，即

$$d \equiv 1^2, \cdots, \left(\frac{p-1}{2}-1\right)^2, \left(\frac{p-1}{2}\right)^2 (\mathrm{mod}\, p).$$

又因为 $1 \le i < j \le \frac{p-1}{2}$ 时，

$$i^2 \neq j^2 (\mathrm{mod}\, p),$$

所以模 p 的二次剩余共有 $\frac{p-1}{2}$ 个．从而知二次非剩余的个数为 $(p-1)-\frac{p-1}{2}=\frac{p-1}{2}$.

从定理 1 的证明知，若方程（2）有解（即 d 为模 p 的二次剩余），则解数为 2．例如当 $p=11$ 时，$d \equiv j^2(\mathrm{mod}11),\ j=1,2,3,4,5$．计算得知 $1,-2,3,4,5$ 为 11 的二次剩余，-1，2，-3，-4，-5 为 11 的二次非剩余．下面我们看一个如何判定 d 为模 p 的二次剩余的定理.

定理 2 (Euler 判别法)设素数 $p>2$，$(p,d)=1$，那么， d 为模 p 的二次剩余的充要条件是

$$d^{(p-1)/2}\equiv 1(\mathrm{mod}\ p);\qquad (1)$$

d 为模 p 的二次非剩余的充要条件是

$$d^{(p-1)/2}\equiv -1(\mathrm{mod}\ p).\qquad (2)$$

证明 对于任意 $d\in Z_p^*$，由 Euler 知

$$d^{p-1}\equiv 1(\mathrm{mod}\ p),$$

所以

$$\left(d^{(p-1)/2}-1\right)\left(d^{(p-1)/2}+1\right)\equiv 0(\mathrm{mod}\ p).$$

从而有

$$d^{(p-1)/2}\equiv 1(\mathrm{mod}\ p)\ \text{或}\ d^{(p-1)/2}\equiv -1(\mathrm{mod}\ p).$$

下证 d 为模 p 的二次剩余的充要条件是 $d^{(p-1)/2}\equiv 1(\mathrm{mod}\ p)$.

必要性：若 d 为模 p 的二次剩余，则存在 x_0 使

$$x_0^2\equiv d(\mathrm{mod}\ p),$$

由 Euler 定理得

$$d^{(p-1)/2}\equiv x_0^{p-1}\equiv 1(\mathrm{mod}\ p).$$

充分性：考虑一次同余方程

$$ax\equiv d(\mathrm{mod}\ p).$$

当 a 取 p 的既约剩余系中某个 j 时，方程有且只有一个解 $x_j(\mathrm{mod}\ p)$．若 d 不为模 p 的二次剩余，则 $j\neq x_j$．可将 p 的既约剩余系按 j,x_j 作为一对两两分完．由 Wilson 定理

$$-1\equiv (p-1)!\equiv d^{(p-1)/2}(\mathrm{mod}\ p).$$

因此与假设矛盾，从而定理得证.

最后证明 d 为模 p 的二次非剩余的充要条件是 $d^{(p-1)/2}\equiv -1(\mathrm{mod}\ p)$.

由 d 为二次剩余的充要条件直接推出 d 为二次非剩余的充要条件为

$$d^{(p-1)/2} \not\equiv -1(\mathrm{mod}\ p).$$

定理得证.

由 Euler 判别法我们很容易得出如下两个推论

推论 1 若 $p \equiv 1(\mathrm{mod}\,4)$，则-1 是模 p 的二次剩余；若 $p \equiv 3(\mathrm{mod}\,4)$，则-1 是模 p 的二次非剩余.

推论 2 设素数 $p > 2$，$(p, d_1) = 1, (p, d_2) = 1$，那么 $d_1 d_2$ 是模 p 的二次剩余的充要条件是 d_1, d_2 均是模 p 的二次剩余或二次非剩余. $d_1 d_2$ 是模 p 的二次非剩余的充要条件是 d_1, d_2 一个为模 p 的二次非剩余，一个为是模 p 的二次剩余.

例 1 求 13 与 23 的二次剩余和二次非剩余.

j	1	2	3	4	5	6
$d = j^2$	1	4	-4	3	-1	-3

所以 $\pm 1, \pm 3, \pm 4$ 是 13 的二次剩余，$\pm 2, \pm 5, \pm 6$ 为二次非剩余.

j	1	2	3	4	5	6	7	8	9	10	11
$d = j^2$	1	4	9	-7	2	-10	3	-5	-11	8	6

所以 $-11, -10, -7, -5, 1, 2, 3, 4, 6, 8, 9$ 是 23 的二次剩余，

$-9, -8, -6, -4, -3, -2, -1, 5, 7, 10, 11$ 是 23 的二次非剩余.

例 2 判断下列同余方程的解数.

（1）$x^2 \equiv 3(\mathrm{mod}\,91)$；　　（2）$x^2 \equiv 4(\mathrm{mod}\,55)$.

解　(1) 同余方程与下列同余方程组同解，

$$\begin{cases} x^2 \equiv 3(\mathrm{mod}\,7) \\ x^2 \equiv 3(\mathrm{mod}\,13) \end{cases}$$

3 不是 7 的二次剩余，所以方程无解，从而 $x^2 \equiv 3(\mathrm{mod}\,91)$ 无解.

(2)　同与方程与同余方程组

$$\begin{cases} x^2 \equiv 4(\mathrm{mod}\,5) \\ x^2 \equiv 4(\mathrm{mod}\,11) \end{cases}$$

同解．4 是 11 的二次剩余，也是 5 的二次剩余，所以原方程的解数为 4．

例 3　d 为模 p 的二次剩余，当 $p\equiv 3(\mathrm{mod}\,4)$ 时，证明 $\pm d^{\,p+1/4}$ 为同余方程

$$x^2\equiv d(\mathrm{mod}\,p)$$

的解．

证明　因为 d 为模 p 的二次剩余，所以

$$d^{\,p-1/2}\equiv 1(\mathrm{mod}\,p)\,.$$

故

$$(d^{\,p+1/4})^2=d^{\,p+1/2}=d^{\,p-1/2}\times d\equiv d(\mathrm{mod}\,p)\,.$$

§6 Legendre 符号与 Jacobi 符号

定义 1　设素数 $p>2$，令

$$\left(\frac{d}{p}\right)=\begin{cases}0, & \text{当}p\mid d\text{时},\\ 1, & \text{当}d\text{为}p\text{的二次剩余时},\\ -1, & \text{当}d\text{为}p\text{的二次非剩余时}.\end{cases}$$

称 $\left(\dfrac{d}{p}\right)$ 为**模 p 的 Legendre 符号．**

定理 1　对于 Legendre 符号有下面的性质：

（1）　$\left(\dfrac{d}{p}\right)=d^{(p-1)/2}\left(\mathrm{mod}\,p\right)$；

（2）　$\left(\dfrac{d}{p}\right)=\left(\dfrac{d+p}{p}\right)$；

（3）　$\left(\dfrac{dc}{p}\right)=\left(\dfrac{d}{p}\right)\left(\dfrac{c}{p}\right)$；

（4）　$\left(\dfrac{-1}{p}\right)=\begin{cases}1, & p\equiv 1(\mathrm{mod}\,4),\\ -1, & p\equiv 3(\mathrm{mod}\,4).\end{cases}$

证明 比较简单留给读者自己证明.

对于一般d，$\left(\frac{d}{p}\right)$的计算一般可以根据性质（1）或后面将要介绍的 Gauss 二次互反律，这两种方法均为较有效的方法．当d 为特殊情况时，如$d=-1$时，$\left(\frac{d}{p}\right)$可以由性质（4）即可求出．当$d=2$，$\left(\frac{d}{p}\right)$的计算可以由下面定理 2 更有效的进行计算.

首先证明一个引理，该引理可以用于证明$\left(\frac{2}{p}\right)$的一个简单的计算公式.

引理 1　设素数 $p>2,\ (p,d)=1$，再设

$$1\le j<p/2,\ t_j\equiv jd(\bmod p),\quad 0<t_j<p\ .$$

以n表示这$(p-1)/2$个t_j中大于 $p/2$ 的t_j的个数，那么

$$\left(\frac{d}{p}\right)=(-1)^n\ .$$

证明 对任意的$1\le j<i<p/2$，

$$t_i\pm t_j\equiv(j\pm i)d\ne 0(\bmod p).$$

即

$$t_i\not\equiv\pm t_j(\bmod p).$$

我们以$r_1,\cdots r_n$表示n个大于 $p/2$ 的t_j，以$s_1,\cdots s_k$表示所有小于 $p/2$ 的t_j，显然$1\le p-r_i<p/2$，又因为

$$s_j\ne p-r_i(\bmod p),\quad 1\le j\le k,\quad 1\le i\le n.$$

所以$s_1,\cdots$，s_k，$p-r_1,\cdots$，$p-r_n$这$(p-1)/2$个数恰好是$1,2,\cdots,(p-1)/2$的一个排列．由题设得

$$1\times 2\times\cdots\times\left((p-1)/2\right)\times d^{(p-1)/2}\equiv t_1t_2\cdots t_{(p-1)/2}$$

$$\equiv s_1\cdots s_k\times r_1\cdots r_n\equiv(-1)^n s_1\cdots s_k\times(p-r_1)\cdots(p-r_n)$$

$$\equiv(-1)^n\times 1\times 2\times\cdots\times\left(\frac{(p-1)}{2}\right)(\mathrm{mod}\,p).$$

从而

$$\left(\frac{d}{p}\right)\equiv d^{(p-1)/2}\equiv(-1)^n(\mathrm{mod}\,p).$$

由引理可得

定理 2 $\left(\dfrac{2}{p}\right)=(-1)^{(p^2-1)/8}$.

证明 因为 $1\le t_j=2j<p/2$，则$1\le j<p/4$，

由引理 1 的证明知 $n=\dfrac{p-1}{2}-\left[\dfrac{p}{4}\right]$. 因此

$$n=\begin{cases}l, & p=4l+1,\\ l+1, & p=4l+3.\end{cases}$$

所以

$$\left(\frac{2}{p}\right)=(-1)^n=\begin{cases}1, & p\equiv\pm1(\mathrm{mod}\,8),\\ -1, & p\equiv\pm3(\mathrm{mod}\,8).\end{cases}$$

定理得证.

引理 2 设素数 $p>2$. 当$(d,2p)=1$时， $(\dfrac{d}{p})=(-1)^T$，其中$T=\sum\limits_{j=1}^{(p-1)/2}[\dfrac{jd}{p}]$.

证明 利用符号整数部分$[x]$，

$$t_j\equiv jd(\mathrm{mod}\,p)，\ 0<t_j<p$$

可表示为

$$jd=p([\frac{jd}{p}]+\{\frac{jd}{p}\})=p[\frac{jd}{p}]+t_j，\ 1\le j<p/2，$$

两边对 j 求和得

$$d\sum_{j=1}^{(p-1)/2} j = p\sum_{j=1}^{(p-1)/2}[\frac{jd}{p}] + \sum_{j=1}^{(p-1)/2} t_j = pT + \sum_{j=1}^{(p-1)/2} t_j \ .$$

由引理 1 的证明知

$$\sum_{j=1}^{(p-1)/2} t_j = s_1 + \cdots + s_k + r_1 + \cdots + r_n$$

$$= s_1 + \cdots s_k + (p - r_1) + \cdots + (p - r_n) - np + 2(r_1 + \cdots + r_n)$$

$$= \sum_{j=1}^{(p-1)/2} j - np + 2(r_1 + \cdots + r_n) \ .$$

由以上两式得

$$\frac{p^2 - 1}{8}(d - 1) = p(T - n) + 2(r_1 + \cdots + r_n) \ .$$

引理 2 得证.

定理 3 （**Gauss 二次互反律**）设 p, q 均为奇素数， $p \neq q$ ，那么

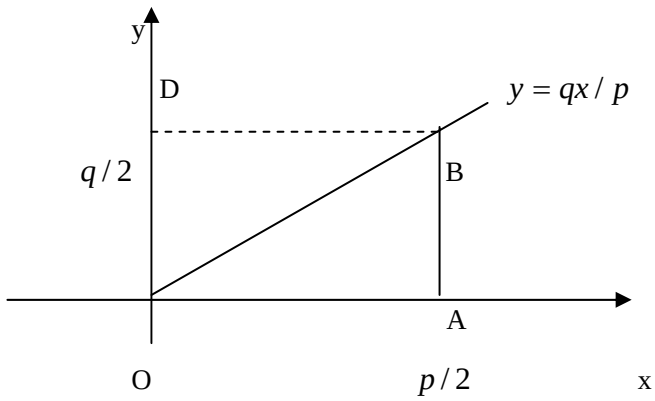
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} \ .$$

证明 由引理 2 得

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{S+T} \ ,$$

其中

$$S = \sum_{i=1}^{(p-1)/2} [\frac{iq}{p}] \ , \quad T = \sum_{j=1}^{(q-1)/2} [\frac{jp}{q}] \ .$$



事实上，S 是

$$y=\frac{q}{p}x,\quad x=\frac{p}{2},\quad y=0$$

三条直线围成区域内部的整点数（不含边界），T 则是

$$y=\frac{p}{q}x,\quad x=\frac{q}{2},\quad y=0$$

三条直线围成区域内部的整点数，略作变形，T 变做

$$y=\frac{q}{p}x,\quad y=\frac{q}{2},\quad x=0$$

三条直线围成区域内部的整点数．于是 $S+T$ 就表示矩形区域

$$x=\frac{p}{2},\quad y=0,\quad x=0,\quad y=\frac{q}{2}$$

内部的整点数（直线 $y=\frac{q}{p}x$ 在此区域不通过整点），即有

$$S+T=\frac{p-1}{2}\frac{q-1}{2}.$$

定理得证．

例 1 计算 $\left(\frac{137}{227}\right)$.

解： 227 是素数

$$\left(\frac{137}{227}\right)=\left(\frac{-90}{227}\right)=\left(\frac{-1}{227}\right)\left(\frac{2\times3^2\times5}{227}\right)=\left(\frac{-1}{227}\right)\left(\frac{2}{227}\right)\left(\frac{3^2}{227}\right)\left(\frac{5}{227}\right)$$

因为

$$227\equiv3(\mathrm{mod}\,4),\quad 5\equiv1(\mathrm{mod}\,4),$$

所以

$$\left(\frac{-1}{227}\right)=-1;\quad \left(\frac{5}{227}\right)=\left(\frac{227}{5}\right)=\left(\frac{2}{5}\right)=-1;$$

由于

$$\left(\frac{2}{227}\right)=(-1)^{p^2-1/8}=-1;\qquad \left(\frac{3^2}{227}\right)=1;$$

因此

$$\left(\frac{137}{227}\right)=-1.$$

例 2　求以 11 为其二次剩余的所有奇素数.

解 由 Gauss 二次互反律

$$\left(\frac{11}{p}\right)=(-1)^{(p-1)/2}\left(\frac{p}{11}\right).$$

直接计算得

$$\left(\frac{p}{11}\right)=\begin{cases}1, & p\equiv 1,-2,3,4,5(\mathrm{mod}11),\\ -1, & p\equiv -1,2,-3,-4,-5(\mathrm{mod}11).\end{cases}$$

$$(-1)^{(p-1)/2}=\begin{cases}1, & p\equiv 1(\mathrm{mod}\,4),\\ -1, & p\equiv 3(\mathrm{mod}\,4).\end{cases}$$

解同余方程组

$$\begin{cases}x\equiv a_1(\mathrm{mod}\,4),\\ x\equiv a_2(\mathrm{mod}11).\end{cases}$$

当 $a_1=1$ 时， a_2 取 1，-2，3，4，5；

当 $a_1=-1$ 时， a_2 取-1，2，-3，-4，-5.

利用孙子定理得 $p\equiv\pm1,\pm5,\pm7,\pm9,\cdots\pm19(\mathrm{mod}\,44)$ 时，

$$\left(\frac{11}{p}\right)=1,$$

即 11 为 p 的二次剩余.

根据 Legendre 符号，我们定义一个更具一般形式的数论函数 Jacobi 符号.

定义 2 设奇数 $P>1, P=p_1,p_2,\cdots p_n, p_i(1\le i\le n)$ 是素数，我们把

$$\left(\frac{d}{P}\right)=\left(\frac{d}{p_1}\right)\left(\frac{d}{p_2}\right)\cdots\left(\frac{d}{p_n}\right)$$

称为 **Jacobi 符号**. 此处 $\left(\frac{d}{p_i}\right),(1\le i\le n)$ 是 **Legendre** 符号.

同样 **Jacobi** 符号也有如下性质：

（1） $\left(\frac{1}{P}\right)=1$；

（2）$(d,P)\neq 1$时，$\left(\frac{d}{P}\right)=0$；

（3）$(d,P)=1$时，$\left(\frac{d}{P}\right)=\pm 1$；

（4） $\left(\frac{d}{P}\right)=\left(\frac{d+P}{P}\right)$；

（5） $\left(\frac{dc}{P}\right)=\left(\frac{d}{P}\right)\left(\frac{c}{P}\right)$；

以上性质由定义 Jacobi 符号可直接推出.

定理 4 （1） $\left(\frac{-1}{P}\right)=(-1)^{P-1/2}$；

（2） $\left(\frac{2}{P}\right)=(-1)^{P^2-1/8}$.

证明 设 $a_i\equiv 1(\mathrm{mod}\, m),(1\leq i\leq s), a=a_1,\cdots a_s$，则

$$\frac{a-1}{m}=\frac{a_1-1}{m}+\cdots+\frac{a_s-1}{m}(\mathrm{mod}\, m).$$

只要证明 $s=2$ 时成立，则其余情况可以类推.

$$a-1=a_1a_2-1=(a_1-1)+(a_2-1)+(a_1-1)(a_2-1),$$

由于 $a_i\equiv 1(\mathrm{mod}\, m)$，所以 $a\equiv 1(\mathrm{mod}\, m)$，从而

$$\frac{a-1}{m}=\frac{a_1-1}{m}+\frac{a_2-1}{m}+\frac{(a_1-1)(a_2-1)}{m}=\frac{a_1-1}{m}+\frac{a_2-1}{m}(\mathrm{mod}\, m).$$

取 $m=2, a_i=p_i\ (1\leq i\leq n)$， $a=P$，由此可以推出

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_n}\right)=(-1)^{(p_1-1)/2+\cdots+(p_n-1)/2}=(-1)^{\frac{P-1}{2}}.$$

同样 $m=4,\ a_i=p_i^{\,2}\left(1\le i\le n\right)$，$a=P^2$，同理可得

$$\left(\frac{2}{P}\right)=(-1)^{(P^2-1)/8}.$$

定理得证.

定理 5 若奇数 $P>1$，$Q>1$，且 $(Q,P)=1$，则

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=(-1)^{(P-1)/2\cdot(Q-1)/2}.$$

证明 设 $Q=q_1\cdots q_s,\ P=p_1\cdots p_t$，则

$$\left(\frac{Q}{P}\right)=\prod_{i=1}^{t}\left(\frac{Q}{p_i}\right)=\prod_{i=1}^{t}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)=\prod_{i=1}^{t}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)(-1)^{(p_i-1)/2\cdot(q_j-1)/2}$$

$$=\left\{\prod_{i=1}^{t}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\right\}\left\{\prod_{i=1}^{t}\prod_{j=1}^{s}(-1)^{(p_i-1)/2\cdot(q_j-1)/2}\right\}$$

$$=\left(\frac{P}{Q}\right)\prod_{i=1}^{t}(-1)^{(p_i-1)/2\cdot\sum_{j=1}^{s}(q_j-1)/2}.$$

由定理 6. 4 的证明知

$$\frac{Q-1}{2}\equiv\sum_{j=1}^{s}(q_j-1)/2\pmod 2,\quad \frac{P-1}{2}\equiv\sum_{i}^{s}(p_i-1)/2\pmod 2.$$

从而

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=(-1)^{(P-1)/2\cdot(Q-1)/2}.$$

利用定理 5 与性质 4 可以计算任何形式的 Jacobi 符号。这实际上是 Euclid 算法的又一个重要应用．特别地，Legendre 符号也可以直接当作 Jacobi 符号来计算.

注：与 Legendre 符号不同的是，Jacobi 符号 $\left(\frac{d}{P}\right)=1$ 并不代表二次同余方程

$$x^2\equiv d\pmod P$$

一定有解.

例 1 求下列 Jacobi 符号 $(\frac{567}{783})$，$(\frac{109}{825})$，$(\frac{281}{633})$.

解 因为 $(567,783)=27>1$，所以 $(\frac{567}{783})=0$；

$$(\frac{109}{825})=(-1)^{(109-1)/2\cdot(825-1)/2}(\frac{825}{109})=(\frac{825}{109})；$$

$$(\frac{109}{825})=(\frac{825}{109})=(\frac{62}{109})=(\frac{2}{109})(\frac{31}{109})=(-1)(\frac{109}{31})=(-1)(\frac{16}{31})=-1；$$

$$(\frac{281}{633})=(\frac{633}{281})=(\frac{71}{281})=(\frac{281}{71})=(\frac{-3}{71})；$$

$$=(\frac{-1}{71})(\frac{3}{71})=(-1)(-1)(\frac{71}{3})=(\frac{2}{3})=-1.$$

习题

1．求解下列同余方程

（1）$4x^2+27x-12\equiv 0(\mathrm{mod}15)$；

（2）$x^2+3x-5\equiv 0(\mathrm{mod}13)$；

（3）$3x^4-x^3+2x^2-26x-2\equiv 0(\mathrm{mod}11)$；

（4）$5x^3-2x^2-7x+6\equiv 0(\mathrm{mod}14)$；

（5）$x^2+8x-13\equiv 0(\mathrm{mod}\,28)$；

（6）$4x^2+9x+2\equiv 0(\mathrm{mod}\,21)$.

2．利用恒等变形解下列同余方程

(1) $x^7+6x^6-13x^5-x^3-2x^2+40x-9\equiv 0(\mathrm{mod}5)$；

(2) $x^9-4x^8-5x^7+x^2+5x+2\equiv 0(\mathrm{mod}\,7)$；

(3) $x^{16}+2x^{15}-5x^{14}+x^{13}-x^4-2x^3+6x^2+2x-5\equiv 0(\mathrm{mod}13)$；

(4) $x^{15}+x^{14}+x^{13}+x^{11}-x^5+2x^4-2x^3+2x^2-27x-2\equiv 0(\mathrm{mod}11)$.

3．设为 p 素数，若 $g(x)\equiv 0(\mathrm{mod}\ p)$ 无解，则 $f(x)\equiv 0(\mathrm{mod}\ p)$ 与

$f(x)g(x)\equiv 0(\mathrm{mod}\ p)$ 的解与解数相同.

4．对哪些值 a，同余方程 $x^3\equiv a(\mathrm{mod}\,9)$ 有解.

5．求 $2^x\equiv x^2(\mathrm{mod}\,3)$ 的解.

6．证明： 同余方程 $f(x)\equiv 0(\mathrm{mod}\,m)$ 的解数为

$$T=\frac{1}{m}\sum_{l=0}^{m-1}\sum_{x=0}^{m-1}e^{2\pi ilf(x)/m}.$$

并由此证明，当 $f(x)\equiv ax-b$ 时，

$$T=\begin{cases}(a,m), & \text{当}(a,m)\mid b;\\ 0, & \text{当}(a,m)\nmid b.\end{cases}$$

7．求解下列一元一次同与方程.

（1）$8x\equiv 6(\mathrm{mod}10)$. （2）$3x\equiv 10(\mathrm{mod}17)$.

（3）$3x\equiv 10(\mathrm{mod}\,29)$. （4）$47x\equiv 89(\mathrm{mod}111)$.

（5）$57x\equiv 87(\mathrm{mod}105)$. （6）$589x\equiv 1026(\mathrm{mod}\,817)$.

8．设 $(a,m)=1,x_1$ 是 $ax\equiv 1(\mathrm{mod}\,m)$ 的解，再设 k 是正整数，$y_k=1-(1-ax_1)^k$.

证明：$a\mid y_k$ 是同余方程的解.

9．设 a 是正整数，$a\nmid m$, 以及 a_1 是 m 对模 a 的最小剩余，证明同余方程 $ax\equiv b(\mathrm{mod}\,m)$ 的解一定是同余方程 $a_1\equiv -b[m/a](\mathrm{mod}\,m)$ 的解，反过来对吗？试用这种方法解同余方程 $6x\equiv 7(\mathrm{mod}\,23)$ 和 $5x\equiv 1(\mathrm{mod}12)$，说明应该注意的问题.

10．解下列同余方程组

1) $\begin{cases}x\equiv 3(\mathrm{mod}\,7)\\ x\equiv 5(\mathrm{mod}11)\end{cases}$;

2) $\begin{cases} x \equiv 1(\mathrm{mod}\,7) \\ 3x \equiv 4(\mathrm{mod}\,5) \\ 8x \equiv 4(\mathrm{mod}\,9) \end{cases}$；

3) $\begin{cases} x \equiv 3(\mathrm{mod}\,8) \\ x \equiv 11(\mathrm{mod}\,20) \\ x \equiv 1(\mathrm{mod}\,15) \end{cases}$；

4) $\begin{cases} x \equiv 3(\mathrm{mod}\,7) \\ 6x \equiv 10(\mathrm{mod}\,8) \end{cases}$；

5) $\begin{cases} x \equiv 7(\mathrm{mod}\,10) \\ x \equiv 3(\mathrm{mod}\,12) \\ x \equiv 6(\mathrm{mod}\,35) \end{cases}$；

6) $\begin{cases} x \equiv 1(\mathrm{mod}\,2^2) \\ x \equiv 0(\mathrm{mod}\,3^2) \\ x \equiv -1(\mathrm{mod}\,5^2) \\ x \equiv -2(\mathrm{mod}\,7^2) \end{cases}$.

1 1．设 $(a.b)=1$，$c \neq 0$，证明：定存在整数 n 使得 $(a+bn,c)=1$.

1 2．证明：同余方程组 $x \equiv a_j(\mathrm{mod}\,m)$，$j=1,2$ 有解的充要条件为 $(m_1,m_2)\,|\,(a_1-a_2)$，若有解，则对模 $m=[m_1,m_2]$ 的解数为一.

1 3．求模为素数幂的同余方程.

(1) $x^2+2x+1 \equiv 0(\mathrm{mod}\,3^2)$；

(2) $x^2+5x+13 \equiv 0(\mathrm{mod}\,3^3)$；

(3) $x^3-2x+4 \equiv 0(\mathrm{mod}\,5^3)$；

(4) $x^3+x^2-4 \equiv 0(\mathrm{mod}\,7^3)$；

(5) $x^5+x^4+1 \equiv 0(\mathrm{mod}\,3^4)$；

(6) $x^2 \equiv 3(\mathrm{mod}\,11^2)$.

1 4．求同余方程的解.

(1) $x^2-10x-11\equiv 0(\mathrm{mod}\,90)$；

(2) $x^2+5x+13\equiv 0(\mathrm{mod}\,54)$；

(3) $x^3-2x+4\equiv 0(\mathrm{mod}\,2\times 5^3)$；

(4) $x^3+x^2-4\equiv 0(\mathrm{mod}\,98)$.

1 5．以 $T_1(m;f)$ 表示同余方程 $f(x)\equiv 0(\mathrm{mod}\,m)$ 满足条件 $(x,m)=1$ 的解数.

证明：$(m_1,m_2)=1$ 时，$T_1(m_1m_2;f)=T_1(m_1;f)T_1(m_2;f)$.

1 6．证明：余方程组 $f(x)\equiv 0(\mathrm{mod}\,m)$，$x\equiv l(\mathrm{mod}\,k)$ 有解的必要条件是

$(m,k)\mid f(l)$.

1 7．设 $m=2^{a_0}p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$，$p_j$ 为不同的奇素数，

$a_j\geq 1(1\leq j\leq r)$，$a_0\geq 0$．证明：余方程 $x_2\equiv 1(\mathrm{mod}\,m)$ 的解数

$$T=\begin{cases}2^r, & a_0=0,1,\\ 2^{r+1}, & a_0=2,\\ 2^{r+2}, & a_0\geq 3.\end{cases}$$

1 8．设 $f(x)$ 是不等于常数的整系数多项式．证明：定存在无数多个素数 p，是同

余方程 $f(x)=0(\mathrm{mod}\ p)$ 有解.

1 9．求 $p=17,19,29,31$ 的二次剩余，二次非剩余.

2 0．验证-3 是否为 67 的二次剩余；11 是否为 53 的二次剩余.

2 1．求下列同余方程的解数.

(1) $x^2\equiv 43(\mathrm{mod}109)$；

(2) $x^2\equiv 7(\mathrm{mod}\,83)$；

(3) $x^2\equiv -5(\mathrm{mod}\,243)$；

(4) $x^2 \equiv 41(\mathrm{mod}1024)$；

(5) $x^2 \equiv 313(\mathrm{mod}\,401)$；

(6) $x^2 \equiv 165(\mathrm{mod}\,503)$.

2 2．设 p 是奇素数，$p \nmid a$．证明：在整数 $u, v, (u,v)=1$，使得

$$u^2 + av^2 \equiv 0(\mathrm{mod}\, p)$$

的充要条件是 $-a$ 是模 p 的二次剩余.

2 3．设 p 是奇素数 $\equiv 1(\mathrm{mod}\,4)$．证明：

（1）$1, 2, \cdots, (p-1)/2$ 中模 p 的二次剩余与非二次剩余的个数均为 $(p-1)/4$ 个；

（2）$1, 2\cdots, p-1$ 中有 $(p-1)/4$ 个偶数为模 p 的二次非剩余，$(p-1)/4$ 个奇数为模 p 的二次非剩余；

2 4．（1）设 p 是奇素数 $\equiv 1(\mathrm{mod}\,4)$，$1,2,\cdots, p-1$ 中全体模 p 的二次剩余之和等于 $p(p-1)/4$；

（2）设 p 是奇素数，证明 $1,2\cdots p-1$ 中全体模 p 的二次剩余之和为

$$S = p(p^2-1))/24 - p\sum_{j=1}^{(p-1)/2}[\frac{j^2}{p}]$$

并用 $17, 19, 29, 31$ 验证.

2 5．利用 Jacobi 符号性质计算.

$(\frac{205}{8633})$，$(\frac{221}{1517})$，$(\frac{105}{341})$，$(\frac{203}{407})$，$(\frac{403}{1519})$，$(\frac{265}{871})$，$(\frac{201}{1769})$.

2 6．（1）求以 7 为其二次剩余的所有奇素数 p；

（2）求以 6 为二次剩余的素数 p；

（3）求以 10 为二次剩余的素数 p.

2 7．素数 $p>2$，证明：$x^4 \equiv -4(\mathrm{mod}\, p)$ 有解的充要条件是 $p \equiv 1(\mathrm{mod}\,4)$.

28.（1）设 $2 \nmid n$，奇素数 $p \mid a^n - 1$，证明：$(\frac{a}{p}) = 1$；

（2）设素数 $p>2$，证明：2^p-1 的素因数 $\equiv \pm 1 (\mathrm{mod}\, 8)$.

29. 设 a,b 是正整数，$2 \nmid b$. 证明：Jacobi 符号有公式

$$\frac{a}{2a+b}=\begin{cases} (\frac{a}{b}), a \equiv 0,1(\mathrm{mod}\, 4) \\ -(\frac{a}{b}), a \equiv 2,3(\mathrm{mod}\, 4). \end{cases}$$

30. 设素数 $p \geq 3$，$p \nmid a$，证明：$\sum_{x=1}^{p}(\frac{x^2+x}{p})=-1$.